

DISEÑADOR,
INTEGRADOR,
OPERADOR DE
SISTEMAS DE MISIÓN
CRÍTICA



El poder de innovación



PRELUDE

PRELUDE SIEM

Monitoreo de Seguridad

PRELUDE es el único sistema SIEM europeo que ofrece una visión unificada en ciberseguridad de sistemas de información. Protege y alerta en tiempo real sobre riesgos y amenazas. Almacena información de trazabilidad para su análisis, investigación y evidencia. Además, ofrece muchas posibilidades de análisis gráfico y matemático permitiendo búsquedas complejas de amenazas persistentes avanzadas (APT).



CARACTERÍSTICAS

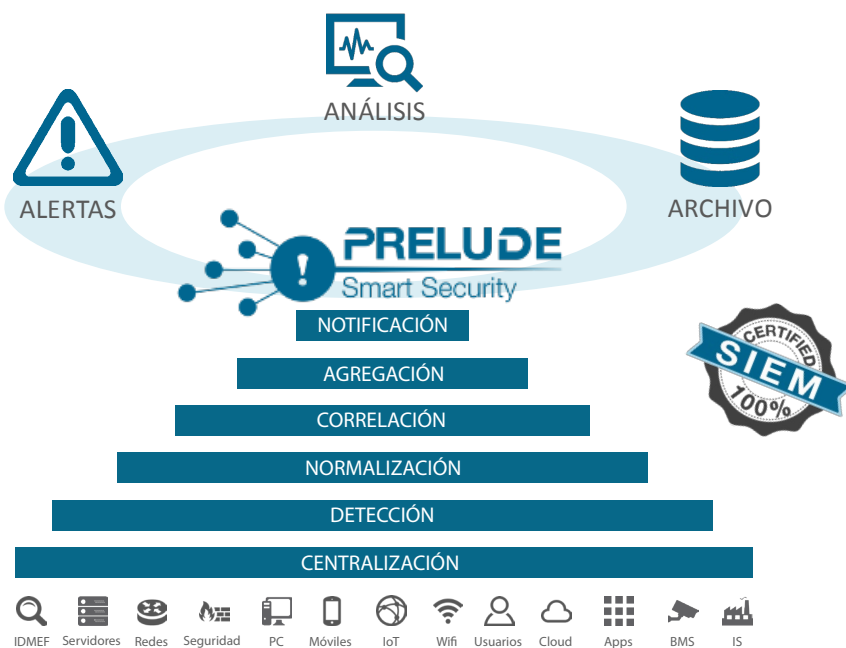
- > Basado en software de código abierto
- > Estándares IDMEF, IODEF
- > Cliente web
- > Big Data: Logs y Netflow
- > Smart Data: correlación inteligente
- > Reportes y cumplimiento de PCI DSS, ISO 27002 y PDIS.
- > Inteligencia de amenazas (Threat intelligence): respuestas, solución multi-tenant, MSSP
- > Fuentes de Log: Syslog, JSON, CEF, LEEF, etc.
- > Arquitectura modular
- > Confidencialidad, enmascaramiento, integridad y trazabilidad



REFERENCIAS

- > Administración, Defensa, Finanzas, Energía, Transporte.
- > Francia, Europa, Canadá, Estados Unidos, América del Sur, África, Asia, Rusia.

www.c-s.fr



ALERTA

La eficiencia del servicio SmartData

PRELUDE identifica comportamientos sospechosos y los muestra en una interfaz con funciones avanzadas de filtrado, clasificación y agregación. Un módulo de gestión de tickets permite la asociación de una alerta con un flujo de trabajo y una base de conocimientos. Este módulo utiliza los formatos estándar IDMEF y IODEF.

ANÁLISIS

Interfaces simples para análisis complejos

El sistema tiene disponibles varias funciones de análisis. Por un lado, el análisis de datos en tiempo real para medir el nivel de criticidad de la situación. Por otro, el análisis de tiempo diferido de información para buscar información oculta en el conjunto de datos. Por último, un módulo permite el análisis forense visual basado en gráficos.

ARCHIVO

Disponibilidad a largo plazo de todos los registros

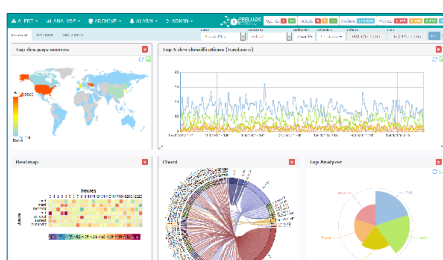
Este módulo archiva todos los logs en una base de datos No-SQL. Gracias a la interfaz avanzada, es posible navegar por los datos archivados para llevar a cabo un análisis post mortem o investigar en una alerta actual con filtros estándares mediante un lenguaje de consulta avanzado tipo «Google».

INTERFACES INTUITIVAS Y AMIGABLES

El significativo trabajo realizado sobre las interfaces de PRELUDE permite facilitar el trabajo diario de los operadores. Sus potentes motores de correlación ayudan a los operadores a identificar amenazas en enormes volúmenes de datos. Tanto las tareas de análisis de eventos y forense, como la investigación de APTs (Advanced Persistent Threats) ahora son más intuitivas y rápidas.

| ID | Name | Severity | Date |
|----|---------------------|----------|----------------|
| 1 | Alerta de seguridad | Alta | 15/05/17 09:23 |
| 2 | Alerta de seguridad | Alta | 15/05/17 09:22 |
| 3 | Alerta de seguridad | Alta | 15/05/17 09:21 |
| 4 | Alerta de seguridad | Alta | 15/05/17 09:20 |
| 5 | Alerta de seguridad | Alta | 15/05/17 09:19 |
| 6 | Alerta de seguridad | Alta | 15/05/17 09:18 |
| 7 | Alerta de seguridad | Alta | 15/05/17 09:17 |
| 8 | Alerta de seguridad | Alta | 15/05/17 09:16 |
| 9 | Alerta de seguridad | Alta | 15/05/17 09:15 |
| 10 | Alerta de seguridad | Alta | 15/05/17 09:14 |

ALERTA



ANÁLISIS

| Fecha | Evento | Severidad | Estado |
|------------------|---------------------|-----------|----------|
| 15/05/2017 09:23 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:22 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:21 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:20 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:19 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:18 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:17 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:16 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:15 | Alerta de seguridad | Alta | Resuelto |
| 15/05/2017 09:14 | Alerta de seguridad | Alta | Resuelto |

ARCHIVO

SERVICIOS



PLAN

Asistencia en la fase de especificación y diseño de su implementación: arquitectura, planificación, recursos, tiempos.



DEPLOY

Brindamos apoyo durante la fase de implementación del SIEM, tanto en modo asistido o «llave en mano».



APPS

Personalización o desarrollo de funciones empresariales específicas para sus propias necesidades.



TRAINING

Capacitación para la configuración y operación de PRELUDE. Entrenamiento basado en escenarios para operadores y empleados.



SERENITY

Soporte personalizado para el manejo del SIEM, mediante reuniones periódicas para asistirlo en la sintonía fina de la herramienta.



EMERGENCY

Nuestro equipo de expertos lo asiste en caso de incidentes o intrusiones para recuperar su actividad tan pronto como sea posible.

www.prelude-siem.com
contact.prelude@c-s.fr

ACERCA DE CS

Como contratista principal en el diseño, integración y operación de sistemas de misión crítica, CS está presente durante toda la cadena de valor de sus clientes. Con una facturación de € 176M y 1.800 empleados, CS es un proveedor reconocido por sus principales clientes gracias a la experiencia y compromiso de su personal.



CS Communication & Systèmes
 22, avenue Galilée - 92350 Le Plessis Robinson
 tél: +33 (0) 1 41 28 40 00 - fax +33 (0) 1 41 28 40 40